Mississippi Department of Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

David C. Johnson, Executive Director

LOC Questions and Clarifications Memorandum

To: Solicited Vendors for Letter of Configuration (LOC) Number 46278, dated February 7, 2023, for the Mississippi State Department of Health (MSDH)

From: David C. Johnson

Date: March 8, 2023

Subject: Responses to Questions Submitted and Clarifications to Specifications

Contact Name: Evan Thiemann

Contact Phone Number: 601-432-8065

Contact E-mail Address: evan.thiemann@its.ms.gov

LOC Number 46278 is hereby amended as follows:

1. **Item 3, PROCUREMENT PROJECT SCHEDULE is hereby amended as follows:**

Task	Date
Addendum with Vendors' Questions and Answers	~~February 21~~March 8, 2023
Proposals Due	~~Tuesday, February 28,~~ Friday, March 17, 2023 at 3:00 p.m. Central Time
Proposal Evaluation	~~February 29,~~ March 20, 2023
Notification of Award	~~March~~ March-April
Contract Negotiations	March-April
Installation	~~March-April~~ April-May
Acceptance	~~April~~ June

2. **Item 4.8 is amended as follows:**

4.8 It is the State's intention that the hardware and software ship to MSDH, Attn: John Wolff at 570 East Woodrow Wilson Dr, Jackson, Mississippi 39201 and be installed on or before ~~April 30,~~ May 30, 2023.

3. **Item 5.6.3 is amended as follows:**

5.6.3 The proposed firewalls shall support at least EIGHTEEN (18) gigabit per second - threat prevention throughput and at least ~~NINE (9)~~ TEN (10) gigabit per second threat prevention Uniform Resource Locator (URL) filtering throughput simultaneously. Vendor must provide 3rd party test reports to substantiate performance (e.g. NSS LABS) with their response.

4. Item 16.1 is hereby revised to read:

16.1 Vendor must deliver the response to Evan Thiemann at ITS no later than ~~Tuesday, February 28~~ Friday, March 17, 2023, at 3:00 P.M. (Central Time). Responses may be delivered by hand, via regular mail, overnight delivery, e-mail, or by fax. Fax number is (601) 713-6380. ITS WILL NOT BE RESPONSIBLE FOR DELAYS IN THE DELIVERY OF PROPOSALS. It is solely the responsibility of the Vendor that proposals reach ITS on time. Vendors should contact Evan Thiemann to verify the receipt of their proposals. Proposals received after the deadline will be rejected.

Vendor must include in their proposal a response to each amended requirement as listed above. Vendor must respond using the same terminology as provided in the original requirements.

The following questions were submitted to ITS and are being presented as they were submitted, except to remove any reference to a specific vendor. This information should assist you in formulating your response.

Question 1: In section 5.1 the list of materials include 2x FG2601 firewalls with a DC power supply. Two lines below there is a request for 4x AC power supplies. Can you provide some clarification on which power supply is needed for these firewalls?

Response: **MSDH/ITS requires the AC power supply in the datacenters.**

Question 2: Can you provide a Visio diagram of your current firewall setup?

Response: **Not at this time. A diagram can be provided to the award vendor after MSDH is in receipt of a non-disclosure agreement.**

Question 3: How many site-2-site tunnel do currently have established? Is this a spilt tunnel?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement. Vendors should be aware that MSDH is in the process of migrating to the State's enterprise VPN solution at this time.**

Question 4: Please specify what MFA/2FA solution is current in place if any.

Response: **Microsoft Authenticator is currently in place. Bidders mays propose an MFA/2FA solution.**

Question 5: There are several methods to perform the migration, and each has advantages and disadvantages. This will help determine the number of cutovers and day-1 support.

Does MSDH have a preference between

(1) Build the new firewalls in parallel and migrate functionality.
(2) Build the new firewalls out-of-band and cutover.
(3) A combination of both methods, depending on Design criteria?

Response: **MSDH prefers option (3) A combination of both methods, depending on Design criteria.**

Question 6: What is MSDH's timeline to have this project fully completed?

Response: **The desire is to have the project completed two months from the date of contract execution.**

Question 7: Would MSDH be open to considering Managed Services for the provisioned Firewalls?

Response: **MSDH is not needed managed services but bidders may propose it.**

Question 8: What are the bandwidth requirements for MSDH?

Response: **MSDH minimum bandwidth requirements: 20G IPS 120G IPV4**

Question 9: Is centralize reporting and management a requirement? If so, do you prefer VM(VMWare or Hyper-V), Cloud(Azure, GCP, AWS), or physical appliances?

Response: **Yes. There is no preference between cloud or physical, but if physical it must be VMWare.**

Question 10: What security services or bundle will need to be enabled on the new firewalls and how many years (1,3, or 5)?

Response: **Refer to Section 5.2. Support is required for a 3 year period.**

Question 11: What is the current firewall model and overall solution?

Response: **Cisco Firepower 2120**

Question 12: How many Interfaces are on the current firewall? (Internal, ISP, DMZ, etc.)

Response: **4**

Question 13: How many current ISP connections exist?

Response: **3**

Question 14: How many current site-to-site (IPSEC) VPNs exist? Indicate intern or external connections.

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement. Vendors should be aware that MSDH is in the process of migrating to the State's enterprise VPN solution at this time.**

Question 15: How many client-to-site VPNs exist? Authentication type?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement. Vendors should be aware that MSDH is in the process of migrating to the State's enterprise VPN solution at this time.**

Question 16: Are you using a RADIUS server? Is it AD as the user database, or LDAP, or NDS?

Response: **Yes, LDAP.**

Question 17: How many existing firewall Rules/Policies?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 18: How many NAT statements exist?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 19: How many Web content filtering profiles?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 20: How many Service Objects?

Response: **Approximately 725**

Question 21: How many Object Groups?

Response: **Approximately 450**

Question 22: How many Static Routes?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 23: How many UTM profiles?

Response: **None**

Question 24: How many User Authentication Sources?

Response: **1 source; at minimum 4 users**

Question 25: Could you provide some sort of network diagram?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 26: What is the timeframe for IPv6 implementation, if not already implemented?

Response: **This is undetermined.**

Question 27: Blurb references “location” of training – is virtual training allowed or does the customer prefer/request “onsite” training?

Response: **MSDH will allow both; virtual is acceptable.**

Question 28: It is noted "up to 10 individuals" may need to be trained. Is this 10 individuals "all at the same time" or would this be spread out across multiple dates/training classes?

Response: **It will be up to 10 individuals at the same time.**

Question 29: Will a link to the Palo (manufacturer) site, listing [Vendor] as an approved Authorized Training Partner, suffice? Or do we need to submit a different type of documentation showing we are authorized to provide Palo training?

Response: **MSDH is seeking Fortinet Appliance, not Palo Alto.**

Question 30: Do you prefer physical or virtual for the Panorama management appliance?

Response: **MSDH is seeking Fortinet Appliance, not Palo Alto.**

Question 31: Do you have a VMware virtualization environment?

Response: **Yes.**

Question 32: Do you want redundancy in the management appliances?

Response: **Yes.**

Question 33: Does this need to be on any sort of state contract?

Response: **No, The awarded vendor will be required to sign a contract with MSDH and ITS as contracting agency.**

Question 34: Would you be able to extend the deadline for this RFP?

Response: **No.**

Question 35: In section 5 Functional/Technical Specifications Item 5.1 the part number for the Fortinet FortiGate firewall is FG-2601F-DC is specified to be located at the ITS Data Center. Does ITS/ MSDH have a DC powered data center?

Response: **No, MSDH/ITS requires AC power supply in the data centers.**

Question 36: What is the hyperscale firewall license to be used for? Typically, this license is used by service providers that don't need Next Gen services on the firewall.

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 37: Are all Next Gen features of the firewalls going to be turned up and used (i.e., web filtering, IDS, IPS, AMP, etc.)?

Response: **Yes.**

Question 38: Will SSL inspection be implemented as part of the installation/configuration project?

Response: **Yes.**

Question 39: Is the requirement for SSL inspection capability to be 10Gbps?

Response: **Yes.**

Question 40: What is the service level and length of support required? Fortinet has 1-, 3- and 5-year FortiCare and FortiGuard with Enterprise Protection, Unified Threat Protection or Advanced Threat Protection. Please specify what is required.

Response: **Refer to Section 5.2. Support is required for a 3 years period.**

Question 41: In the LOC Technical Specifications section 5.1 and 5.2 lists the components that are request, or equivalent and it appears MSDH is looking to procure Next Generation Firewalls to and leverage Hyperscale. Can ITS or MSDH outline how the traffic flow is intended to be setup for installation purposes?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

Question 42: The provided equipment list in 5.1 and 5.2 does not include any subscription/licenses/feeds for Fortinet's UTM functionality; however, the technical specifications in section 5.6.3, 5.6.4, 5.6.7, 5.11, 5.12, 5.13, 5.16 are written around throughputs and specifications that would require these additional licenses. Do these licenses need to be added or should the specifications be adjusted?

Response: **The pricing should be included as part of the appliance proposal.**

Question 43: In section 5.6.3 it states 9 GBs for Threat and URL and in section 5.6.4 it states 10 GBs for all services, when all services are enabled, is better performance expected or is there a throughput amount that can be shared that the solution should meet?

Response: **Minimum requirements: 10gbps. Please refer to the amended specifications at the beginning of this document.**

Question 44: In Section 5.6.10 modern malware protection. Is there a required throughput performance for this feature?

Response: **No.**

Question 45: In section 5.8 through 5.8.5 is specifications around High Availability (HA) however in section 5.6.1 the LOC states that one of the two firewalls shall be an offline spare. Will the second firewall be setup in HA or setup as an offline spare?

Response: **It will be setup in HA.**

Question 46: In section 5.6.8 it calls out the solution shall include special ASIC to handle signature matching and processing in a single pass parallel processing architecture. This requirement is specific to a single manufacture. Is ITS and MSDH open to solutions that handle this as efficiently/effectively, but in a different process?

Response: **Yes, MSDH is open to different solutions that handle this in an equivalent manner.**

Question 47: In section 5.9.1 states the proposed firewall solution shall support a centralized management server for enterprise management of the firewall devices. Is it acceptable for this to be managed from the cloud?

Response: **Yes.**

Question 48: In section 5.6.11 it states the proposed firewalls shall support multiple logically separated virtual systems of context on a physical firewall up to 20 virtual firewalls. Are 20 virtual firewalls a requirement or can the state share the actual number of contexts that are required for the agency?

Response: **MSDH will provide this information to the awarded vendor upon execution of non-disclosure/confidentiality agreement.**

If you have any questions concerning the information above or if we can be of further assistance, please contact Evan Thiemann at 601-432-8065 or via email at evan.thiemann@its.ms.gov.

cc: ITS Project File Number 46278